REMARKS

Claims 1-21 are pending in the present application. Claims 1, 8, and 15 were amended to recite the feature of calculating a severity level for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group. Support for these amendments may be found at least one page 12, line 29 to page 13, line 7. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 103, Obviousness, Claims 1-21

The examiner has rejected claims 1-21 under 35 U.S.C. § 103 as being unpatentable over Farley et al. (Publication Number: 2002/0078381), in view of Burrows et al. (Publication Number 2002/0073338). This rejection is respectfully traversed.

With regard to claims 1, 8, and 15, the examiner states:

> As per claim 1, 8, and 15, Farley teaches a method in a data processing system for reporting security situations, comprising the steps of:
>
> Logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute (Farley, see example, Para [0019] Line 1-3 and Para [0019] Line 12-17: SRC/DEST/EVENT TYPE as the event attribute parameters);
>
> Farley teaches classifying and correlating the raw events (Farley, Para [0019] Line 1-3). However, Farley does not disclose expressly classifying events as groups by aggregating events with at least one attribute within the event set as an identical value.
>
> Burrow teaches classifying events as groups by aggregating events with at least one attribute within the event set as an identical value (Burrows, see example, Para [0050] and Para [0046] Line 10-11: Burrows teaches aggregating the correlated raw events into event groups with at least one attribute within the event set as an identical value such as (a) same SRC address (Para [0050]), or (b) same DEST address (Para [0046] Line 10-11) to detect broadcasting traffic storm and server attached network problems respectively).
>
> calculating severity levels for the groups (Burrows: Para [0050] Line 3-9: the "broadcast storm" is qualified to meet the severity level as an event caused by the identical SRC and different DEST when the aggregating events exceed the predetermined number (i.e., threshold) as taught by Burrows).
>
> reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value (Burrows: Para [0050] Line 3-9 and Para [0018] Lin 14-17: instructing the switches to discard packets or disable the forwarding SRC port accordingly, as an appropriate action of the problem reports).
>
> It would have been obvious to a person of ordinary skill in the art at the

> time the invention was made to combine the teaching of Burrows within the system of Farley because (a) Farley teaches classifying and correlating raw events by providing a security management system in a network computer system (Farley, Para [0019] Line 1-3 and Para [0016] and (b) Burrows teaches improving network throughput performance by recognizing undesirable packet traffic patterns after aggregating the correlated raw events into event groups such as broadcasting traffic storm and server attacked group event (Burrows, see example, Para [0050] and Para [0046] Line 10-11).

Office Action dated October 3, 2005, Pages 3-5.

The examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). To establish a *prima facie* case of obviousness, the examiner must show some suggestion or motivation to combine or modify reference teachings, show a reasonable expectation of success, and show that the cited references teach or suggest all of the claim limitations. MPEP § 706.02(j).

Amended independent claim 1, which is representative of amended independent claims 8 and 15 with regard to similarly recited subject matter, reads as follows:

> 1. A method in a data processing system for reporting security situations, comprising the steps of:
>
> logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;
>
> classifying events as groups by aggregating events with at least one attribute within the event set as an identical value;
>
> calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group; and
>
> reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

Applicants agree with the examiner that *Farley* does not teach classifying events as groups by aggregating events with at least one attribute within the event set as an identical value. As *Farley* does not teach or suggest classifying events a groups, *Farley* does not teach or suggest calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group, nor does the examiner allege that any section of *Farley* does so.

Burrows does not cure the deficiencies of *Farley*. The examiner alleges that Burrow

teaches calculating a severity level for the groups in the following cited passage below:

> Observing more than a predetermined number of broadcast packets within a predetermined time period implies that a broadcast storm is underway. It is likely that the packet is correctly addressed, and that knowing the source MAC address and the network topology will point to a particular port of a forwarding device, e.g., switch port, to be disabled.

Burrows, paragraph [0050], lines 3-9.

The passage above discloses that a packet traffic monitor observes network traffic. When more than a predetermined number of broadcast packets are observed within a predetermined time period, it is determined that a broadcast storm or continuous stream of packets have been emitted. The source MAC address of the packets may then be used when taking action against the broadcast storm, such as disabling the port associated with the offending host to limit the number of broadcast packets.

However, the passage above does not teach calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group. The passage merely teaches using a predetermined threshold value when monitoring a network. The threshold value is used to determine if more than a predetermined number of broadcast packets have been observed within a predetermined amount of time. There is no discussion in *Burrows* of calculating a severity level as recited in the claimed invention. The examiner alleges that "the 'broadcast storm' is qualified to meet the severity level as an event cause by the identical SRC and different DEST when the aggregating events exceed the predetermined number (i.e., threshold)". However, determining if the number of broadcast packets observed is above a predetermined amount or threshold value is not the same as calculating the severity level for a group. Instead, observing multiple packets within a time period in *Burrows* is akin to identification of an event, rather than calculating severity. The severity level as recited in the claim invention is a function of a number of events comprising the group and values of common elements in the group. Thus, the common elements in the group have values which are used to calculate the severity level of the group. While *Burrows* uses the number of broadcast packets within a time period to determine whether or not a broadcast storm is underway, there is no mention in *Burrows* of having values of common elements in the group, much less calculating the severity levels of the group based on the values of common elements in

the group. *Burrows* merely discloses observing broadcast packets, and disabling a port when the number of observed packets exceed a threshold value.

Thus, while *Burrows* may use a threshold to determine whether or not the observed broadcast packets should be limited or not, *Burrows* does not teach or suggest anything about calculating a severity level that is based on a number of events comprising the group and values of common elements in the group. Even if the missing elements of the rejected claims existed in the prior art, for the rejected claims to be obvious there must be some motivation or incentive from the prior art to modify or combine the reference teachings to achieve the present invention. The examiner does not provide any motivation from either reference that making all the necessary modifications to the reference teachings to achieve the present invention would be desirable. If the examiner cannot make such a showing, then the examiner has simply relied on hindsight with the benefit of applicants' disclosure to develop an incentive for the changes, which in fact, would not be obvious to one of ordinary skill in the art at the time the invention was made.

In view of the above, applicants submit that independent claims 1, 8, and 15 are not taught or suggested by the alleged combination of *Farley* and *Burrows*. At least by virtue of their dependency on claims 1, 8, and 15, respectively, *Farley* and *Burrows* also do not teach or suggest the features in dependent claims 2-7, 9-14, and 16-21. Furthermore, claims 2-7, 9-14, and 16-21 recite additional subject matter not suggested by the *Farley* and *Burrows* references. For instance, claims 2, 9, and 16 recite severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups. As discussed in the response to the rejection of claims 1, 8, and 15 above, the features of calculating the severity levels in these claims are neither taught nor suggested by *Farley* or *Burrows*. Accordingly, applicants respectfully request withdrawal of the rejection of claims 2-7, 9-14, and 16-21 under 35 U.S.C. §103.

Therefore, the rejection of claims 1-21 under 35 U.S.C. § 103 has been overcome.

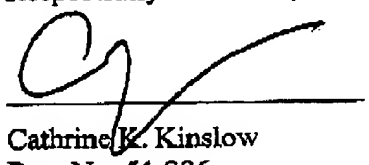
II. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: December 13, 2005

Respectfully submitted,



Cathrine K. Kinslow
Reg. No. 51,886
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants